Docket No. 99-064 MIS

CLAIMS:

What is claimed is:

Sub A1

1. An encryption key management system comprising:

a master key; and

a portable processor, wherein the portable processor uses the master key for generating an encryption key.

2. The encryption key management system recited in claim 1 further comprising:

a variable key range variable, wherein the portable processor further uses the variable key range variable for generating the encryption key.

Sub A2

3. The encryption key management system recited in claim 2, wherein the variable key range variable is output with the encryption key.

4. The encryption key management system recited in claim 2, wherein the variable key range variable comprises at least one of a card number, a card group number and a reference number representing a number of keys.

5. The encryption key management system recited in claim 2, wherein the portable processor further comprises:

a hashing function for generating the encryption key.

6. The encryption key management system recited in claim 1, wherein the portable processor is a smart card.

7. The encryption key management system recited in claim 6, wherein the smart card is accessed through verification of a personal identification number.

8. The encryption key management system recited in claim 4, wherein the portable processor further comprises:

an incrementor for increasing the value of the reference number in response to the encryption key being generated.

9. The encryption key management system recited in claim 1, wherein the portable processor is a first portable processor and the system further comprises:

a second portable processor, wherein the portable processor uses the master key for generating a decryption key.

10. The encryption key management system recited in claim 9, wherein the second portable processor further uses the variable key range variable for generating the encryption key.

11. The encryption key management system recited in claim 10, wherein the variable key range variable is input to the second portable processor.

12. The encryption key management system recited in claim 10, wherein the second portable processor further comprises:

a hashing function for generating the decryption key using the master key.

13. The encryption key management system recited in claim 9, wherein the second portable processor is a smart card.

14. The encryption key management system recited in claim 13, wherein the smart card is accessed through verification of a personal identification number.

15. The encryption key management system recited in claim 10, wherein the second portable processor further comprises:

a hashing function for generating the decryption key.

16. An encryption key management system comprising:

a master key; and

a portable processor, wherein the portable processor uses the master key for generating a decryption key.

17. The encryption key management system recited in claim 16 further comprising:

a variable key range variable, wherein the portable processor further uses the variable key range variable for generating the decryption key.

Sub A3

~~18. The encryption key management system recited in claim 17, wherein the variable key range variable is output with the decryption key.~~

~~19. The encryption key management system recited in claim 16, wherein the variable key range variable comprises at least one of a card number, a card group number, and a reference number representing a number of keys.~~

Sub A4

~~20. The encryption key management system recited in claim 17, wherein the portable processor further comprises:~~

~~a hashing function for generating the decryption key.~~

~~21. The encryption key management system recited in claim 16, wherein the portable processor is a smart card.~~

~~22. An encryption key management method comprising:~~

~~receiving a master key;~~

~~generating an encryption key using the master key, wherein the encryption key is generated by a portable processor; and~~

~~outputting the encryption key.~~

~~23. The method recited in claim 22 prior to generating an encryption key the method further comprises:~~

~~creating a variable key range variable, wherein the portable processor uses the variable key range variable for generating the encryption key.~~

Sub A5

~~24. The method recited in claim 23 further comprises:~~
~~outputting the variable key range variable.~~

~~25. The method recited in claim 23, wherein the variable key range variable comprises at least one of a card number, a card group number, and a reference number representing a number of keys.~~

Sub A6

~~26. The method recited in claim 23, wherein generating the encryption key further comprises:~~
~~hashing the master key.~~

~~27. The method recited in claim 23, wherein the portable processor is a smart card.~~

~~28. The method recited in claim 27 further comprises:~~
~~verifying a personal identification number; and~~
~~accessing functionality of the smart card.~~

~~29. The method recited in claim 22, wherein the portable processor is a first portable processor and the method further comprises:~~
~~generating a decryption key using the master key, wherein the decryption key is generated by a second portable processor; and~~
~~outputting the decryption key.~~

~~30. The method recited in claim 29, prior to generating the encryption key further comprises:~~

receiving a variable key range variable, wherein the second portable processor uses the variable key range variable for generating the encryption key.

31. The method recited in claim 23, wherein the second portable processor is a smart card.

32. The method recited in claim 22, wherein a smart card is accessed through verification of a personal identification number.

33. An encryption key management method comprising:

receiving a master key; and

generating a decryption key using the master key, wherein the decryption key is generated by a portable processor; and

outputting the decryption key.

34. The method recited in claim 33 prior to generating the decryption key the method further comprises:

creating a variable key range variable, wherein the portable processor uses the variable key range variable for generating the decryption key.

Sub A7

35. The method recited in claim 34 further comprises:

outputting the variable key range variable.

36. The method recited in claim 34, wherein the variable key range variable comprises at least one of a card number,

a card group number, and a reference number representing a number of keys.

Sub A8

37. The method recited in claim 34, wherein generating the decryption key further comprises:

hashing the master key.

38. The method recited in claim 34, wherein the portable processor is a smart card.